McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Christine Czuprynski
Direct Dial: 248-220-1360
E-mail: cczuprynski@mcdonaldhopkins.com

August 29, 2019

VIA U.S. MAIL

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Central Michigan University – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Central Michigan University. I am writing to provide notification of an incident at Central Michigan University that may affect the security of personal information of approximately three (3) Maryland residents. Central Michigan University's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Central Michigan University does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Central Michigan University recently learned that an unauthorized individual may have obtained access to multiple Central Michigan University email accounts between December 7, 2018 and March 14, 2019. Central Michigan University immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the email account and the security of the emails and attachments contained within it. Following the extensive forensic investigation and manual document review, we discovered on August 1, 2019 that the impacted email accounts contained personal information belonging to a limited number of individuals, including the affected residents' full names and driver's license numbers. Residents' Social Security numbers were not impacted.

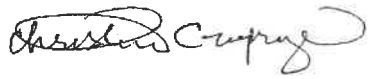
To date, Central Michigan University is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Central Michigan University wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Central Michigan University is providing the affected residents with written notification of this incident commencing on or about August 30, 2019 in substantially the same form as the letter attached hereto. Central Michigan University is advising

the affected residents about the process for placing fraud alerts and/or security freezes on credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission, and the Maryland Attorney General.

At Central Michigan University, protecting the privacy of personal information is a top priority. Central Michigan University is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Central Michigan University continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Christine Czuprynski

Encl.

Central Michigan University
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

Central Michigan University

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

August 30, 2019

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to Central Michigan University ("CMU"). As such, we wanted to provide you with information about a privacy incident at CMU and let you know that we continue to take significant measures to protect your information.

What Happened?

CMU has learned that multiple CMU employees may have been the victims of an email phishing attack, resulting in unauthorized access to those employees' email accounts.

What We Are Doing.

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we worked very closely with external cybersecurity professionals. The forensic investigation concluded that multiple CMU email boxes may have been accessed by an unauthorized party from December 7, 2018 to March 14, 2019. Following the extensive forensic investigation and manual document review, we discovered on August 1, 2019 that the impacted email accounts contained personal information belonging to a limited number of individuals, including you. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The impacted email accounts that were accessed may have contained some of your personal information, including your full name and driver's license number.

What You Can Do.

This letter provides precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We regret any inconvenience you may experience as we are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and have already modified our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available [redacted].

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial 1-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the CMU in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts.

You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.